

**REMARKS**

A review of the claims indicates that:

A) Claims 1—82 are cancelled.

B) Claims 83—124 are new.

In view of the following remarks, Applicant respectfully requests allowance of the new claims.

**Discussion of §103 Issues**

Claims 83—124 are new. Full support for these claims is found in Figs. 3 and 4, in the discussion of these figures, and in other locations. In order to move the prosecution of this application forward, the Applicant addresses §103 issues associated with U.S. Patent No. 6,079,018 (hereinafter “Hardy”) and U.S. Patent No. 6,453,416 (hereinafter “Epstein”).

**The §103 Standard**

To establish a *prima facie* case of obviousness, three basic criteria *must* be met. MPEP § 2142. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992); *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Second, there must be a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Hence, when patentability turns on the question of obviousness, the search for, and analysis of, the prior art includes evidence relevant to the finding of

1 whether there is a teaching, motivation, or suggestion to select and combine or  
2 modify the references relied on as evidence of obviousness. The need for  
3 specificity pervades this authority. See, e.g., *In re Kotzab*, 217 F.3d 1365, 1371,  
4 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) ("particular findings must be made as to  
5 the reason the skilled artisan, with no knowledge of the claimed invention, would  
6 have selected these components for combination in the manner claimed").

### 7 Discussion of §103 Issues

8 The Applicant herein addresses issues related to the Section 103 rejection  
9 of Claim 3 that may be relevant to the new claims.

10 **Claim 83** recites a method, at least partially implemented by a computer,  
11 comprising:

- 12 • **building a data block comprising a first random value and a  
cryptographic hash of the first random value;**
- 13 • generating, on a second computing device, a signature by digitally  
signing a string containing a second random value; and
- 14 • computing an encryption key, for encrypting the data block, by  
hashing a combination of the signature and a third random value.

15 The Hardy reference discloses five (5) embodiments for generating unique  
16 secure values for digitally signing documents. In none of these embodiments does  
17 Hardy teach or suggest building a data block comprising a first random value and  
18 a cryptographic hash of the first random value. In particular, Hardy teaches the  
19 Prior Art method for signing documents, at FIG. 1. Additionally, Hardy teaches  
20 four embodiments—seen at FIGS. 3 through 6—that teach Hardy's advancements  
21 in this area.  
22

23 Hardy's advancements include a method of deriving a pseudo random key,  
24 known as "k". The pseudo random key k is mentioned at column 8, lines 22—23,  
25

1 and is seen as the “middle variable” input to the signature generation procedure  
2 148. (Note that this procedure is mentioned without the typo seen in the FIGS.  
3 3—6 of the drawings at column 10, lines 45—46 and other locations.) In  
4 operation, k is used along with a private key “x” and a hash “H” of the document  
5 in a known “signature generating procedure” (e.g. DSA) to create a “digital  
6 signature”.

7 Hardy does not teach or suggest, “building a data block comprising a first  
8 random value and a cryptographic hash of the first random value”. The Applicant  
9 will now review the locations wherein Hardy teaches the use of random values,  
10 and the locations wherein Hardy teaches hashed values. By way of this review, it  
11 will be seen that Hardy does not teach or suggest the combination of a random  
12 value and the hash of the random value in a data block.

14 Referring to the Hardy reference, Hardy uses random values in several  
15 locations. In FIG. 1, Hardy teaches that the key “k” can be random (see Hardy,  
16 column 1, lines 60—65). In operation, Hardy pairs the key “k” with the private  
17 key “x” and the hash of the document (not the hash of the key “k”). Thus, Hardy  
18 uses these values as input to the digital signature algorithm, and does not teach or  
19 suggest *creation of a data block comprising a random value and a hash of the*  
20 *random value.*

22 Referring to FIG. 3 of Hardy, creates the key k1, which appears to be the  
23 same as the pseudo random key k of FIG. 1. However, Hardy pairs the key “k1”  
24 with the hash H of the document 52. Thus, Hardy does not teach or suggest  
25

1 forming a data block with a random value and its hash. Instead, Hardy creates  
2 “k1” and pairs it with the hash *of the document*. Thus, Hardy does not teach the  
3 random value and the hash of the random value. Moreover, Hardy does not  
4 disclose creation of a data block; instead, Hardy teaches using the values as input  
5 to the hash procedure 146.

6 Continuing to refer to FIG. 3, Hardy additionally teaches the creation of the  
7 pseudo random key “k”. However, Hardy teaches (same as FIG. 1) that the key  
8 “k” is combined with the hash of the document “H” and the private key “x”.  
9 These three data are used as input to the signature generating procedure 148.  
10 Thus, Hardy does not teach, “building a data block comprising a first random  
11 value and a cryptographic hash of the first random value”.  
12

13 Referring to FIGS. 4—6 of Hardy, it can be seen that Hardy continues to  
14 teach that a random or pseudo random value (e.g. “k”) can be combined with a  
15 hashed value. However, Hardy fails to teach a data block having a random value  
16 and a hash of that random value. For example, while Hardy teaches that “k” can  
17 be a random value, Hardy fails to teach or suggest that “k” can be combined with  
18 the hash of “k” to form a data block. Instead, “k” is used with the hash “H” of the  
19 document 52.  
20

21 In the rejection of Claim 3, the Patent Office suggested that the random  
22 value “k” and the hash “H” (by hash procedure 146) of the document 52 taught  
23 and/or suggested the elements of the Applicant’s claim. The Applicant  
24 respectfully disagrees.  
25

1 In fact, Claim 83 recites, a data block comprising “a first random value and  
2 a cryptographic hash of the first random value”. That is, the data block includes a  
3 random value and a cryptographic hash of *that* random value.

4 In contrast, as the Patent Office points out, Hardy teaches that the random  
5 value “k” is combined with the hash “H” of the document—and not with the hash  
6 of “k”. In fact, Hardy does not teach that “k” is hashed, let alone that the hash of  
7 “k” is combined with “k”.

8 Therefore, Hardy does not teach or suggest, “building a data block that  
9 includes a first random value and a cryptographic hash of the first random value”.  
10 Accordingly, the Applicant respectfully requests that the Patent Office withdraw  
11 the argument against original Claim 3, and allow new Claim 83 and its dependent  
12 claims.  
13

14 **Claims 84—91** depend from Claim 83 and are allowable as depending  
15 from an allowable base claim. These claims are also allowable for their own  
16 recited features that, in combination with those recited in Claim 84, are neither  
17 disclosed nor suggested in references of record, either singly or in combination  
18 with one another.  
19  
20  
21  
22  
23  
24  
25

1 **Claim 92** recites a method, at least partially implemented by a computer,  
2 comprising:

- 3 • accessing an encrypted data block, **wherein the encrypted data**  
4 **block comprises an encryption of a combination of a first**  
5 **random value and a hash of the first random value;**
- 6 • accessing second and third random values;
- 7 • providing a string containing the second random value to a second  
8 computing device;
- 9 • generating, on the second computing device, a signature by digitally  
10 signing the string containing the second random value; and
- 11 • computing a decryption key, configured to decrypt the encrypted  
12 data block, wherein computing the decryption key uses the signature  
13 generated on the second computing device and the third random  
14 value.

15 As seen in the discussion of Hardy, above with respect to Claim 83, Hardy  
16 does not teach or suggest a data block comprising “an encryption of a first random  
17 value and a hash of the first random value”. Instead, Hardy teaches random  
18 values, such as the pseudo random key “k”. Additionally, Hardy teaches use of a  
19 hash function. For example, (referring to FIG. 3) Hardy teaches that the document  
20 52 is hashed and that the intermediate value “k2” is hashed to result in the pseudo  
21 random key “k”.

22 However, Hardy does not teach accessing an encrypted data block, wherein  
23 the encrypted data block comprises an encryption of a random value *and a hash of*  
24 *that random value.*

25 As seen above in the discussion of Claim 83, in addressing rejection of  
Claim 3, the Patent Office suggests that the association of the random key “k” and  
the hash “H” of the document 52 meets the elements recited in the claims.  
However, the Applicant must respectfully disagree.

1 In fact, the document 52 is different from the key "k". Therefore, the hash  
2 of "k" will be different from the hash "H" of the document 52. Accordingly, the  
3 combination of the key "k" and the hash of the document 52 is not the same as  
4 would be the case if Hardy had taught or suggested combining the key "k" with  
5 the hash of the key "k". However, such a step would not fit into the algorithm  
6 taught by Hardy, nor would Hardy's algorithm suggest such as step. In fact, there  
7 is no use for the hash of the key "k" in Hardy's algorithm, and Hardy does not  
8 teach or suggest that "k" be hashed, let alone hashed and combined with "k" in a  
9 data block.  
10

11 Accordingly, Hardy does not teach or suggest a data block comprising an  
12 encryption of a first random value and a hash of that value.

13 In the prior Office Action, the Patent Office addressed this issue with  
14 respect to Claim 3. The Applicant respectfully disagrees with the Patent Office's  
15 conclusions. Accordingly, the Applicant incorporates herein, by reference, the  
16 discussion seen with respect to Claim 83, above.  
17

18 Therefore, Hardy does not teach or suggest, "accessing an encrypted data  
19 block, wherein the encrypted data block comprises *an encryption of a first random*  
20 *value and a hash of the first random value*". Accordingly, the Applicant  
21 respectfully requests that the Patent Office allow Claim 92 and its dependent  
22 claims.  
23

24 **Claims 93—96** depend from Claim 92 and are allowable as depending  
25 from an allowable base claim. These claims are also allowable for their own

1 recited features that, in combination with those recited in Claim 92, are neither  
2 disclosed nor suggested in references of record, either singly or in combination  
3 with one another.

4 **Claims 97—124** are allowable for at least the reasons that claims 83—96  
5 are allowable.

6 **Conclusion**

7 The arguments presented above are intended to present the Applicant's  
8 position clearly, but should not be considered exhaustive. Accordingly, the  
9 Applicant reserves the right to present additional arguments to clarify the  
10 Applicant's position further. Moreover, the Applicant reserves the right to  
11 challenge the status as prior art of one or more documents cited in the Office  
12 Action.  
13

14 The Applicant submits that the claims as presented are in condition for  
15 allowance. Accordingly, the Applicant respectfully requests that a Notice of  
16 Allowability be issued. If the Patent Office's next anticipated action is not the  
17 issuance of a Notice of Allowability, the Applicant respectfully requests that the  
18 undersigned attorney be contacted to schedule an interview.  
19

20  
21 Respectfully Submitted,

22 Dated: 2-13-06

23 By: 

24 David S. Thompson  
25 Reg. No. 37,954  
Attorney for Applicant



LEE & HAYES PLLC  
Suite 500  
421 W. Riverside Avenue  
Spokane, Washington 99201  
Telephone: 509-324-9256 x235  
Facsimile: (509) 323-8979

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25